Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 19 August 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Detroit Free Press reports for the fifth day in a row, Detroit Water and Sewerage Department officials are asking their 4.3 million customers to boil all tap water before drinking it. (See item 14)
- The Chicago Sun Times reports last week's blackout disrupted emergency dispatch systems in Detroit and New York, leaving 911 operators to write notes to distribute to police officers on the streets, and cutting communications between dispatchers and personnel for spans as long as 14 minutes. (See item 20)
- Department of Homeland Security has issued advisory "New version of the MS−RPC DCOM Worm infecting machines and creating Denial of Service." (See item 24)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 18, The Straits Times (Singapore)* — **U.S. electrical grid vulnerable to terrorism. A growing number of security experts in and out of the U.S. government are worried that potentially hostile states and even a rebuilt al Qaeda could wreak havoc through simultaneous and coordinated assaults on sensitive points on the electrical grid.** Industry officials said that during the second half of last year, 60 per cent of the country's power and

energy companies experienced hacking attacks, however, none were successful. According to Steven Flynn, a senior fellow on the Council on Foreign Relations, the grid has many other vulnerabilities. If the electrical transformer for the Port of Los Angeles and Long Beach in California were blown up, for instance, it could take months, even under a crash programme, to bring electricity back to the vital port facility, which handles more than 30 per cent of the nation's imports in terms of dollar value. There are no spare transformers, he said, and it normally takes two years from order to delivery for a new one, and most are built in South Korea.
Source: http://www.straitstimes.asia1.com.sg/world/story/0,4386,2053 39,00.html?

2. *August 18, The Associated Press* — **Phoenix gas stations running dry after pipeline shut down.** The gas pipeline between Phoenix and Tucson, AZ, ruptured July 30, spilling about 12,000 gallons of fuel, and the operator shut it down August 8 because of concerns that there could be more problems. Since then, **gas has been trucked up from Tucson, and AAA has been urging drivers not to panic.** Executives of Kinder Morgan Energy Partners, the Houston company that operates the pipeline, got approval from federal regulators Thursday, August 14, for their plan to repair the line and test it for safety. But company officials say it would be one or two weeks before the pipeline is running again. **About 70% of the gas Phoenix uses comes from California, and the rest from Texas, and all of it comes from Tucson through the single pipeline.**
Source: http://www.usatoday.com/news/nation/2003−08−18−phoenix−gas_x .htm

3. *August 18, Reuters* — **Progress Energy shuts North Carolina nuke. Progress Energy Inc. said it manually tripped its 900 megawatt Harris nuclear unit on Sunday, August 17, the Nuclear Regulatory Commission said in its power reactor status report.** The company manually tripped the reactor due to a trip of a condensate pump and subsequent trip of a main feed pump. The company, which is investigating the cause of the shutdown, said the condensate pump may have tripped due to an electrical storm. The Harris station is twenty miles southwest of Raleigh, NC.
Source: http://biz.yahoo.com/rm/030818/utilities_progress_harris_1.h tml

4. *August 18, Dow Jones Business News* — **Blackout exposes power companies to potential lawsuits. The biggest blackout in U.S. history looks set to trigger a flood of lawsuits against power companies.** As of now, there is no conclusion that any one company is to blame for the power failure. But a preliminary finding by the North American Electric Reliability Council identified FirstEnergy Corp. as a likely source of the outage. There could be "tens of thousands" of lawsuits filed against FirstEnergy and others as a result of the power failure, said Dick Pierce, a law professor at George Washington University in Washington. **States, businesses and individuals could sue to recoup economic losses, he added, and some utilities may file suits against other utilities in an effort to shift the blame.** Insurance companies may also sue to recover the money they pay out for claims.
Source: http://biz.yahoo.com/djus/030818/1542000857_1.html

5. *August 18, The Associated Press* — **Power swings seen hours before blackout. The Midwest power system recorded numerous voltage swings as early as midday Thursday, August 14, long before high−voltage lines failed south of Cleveland, OH, officials said.** This raised new questions of what might have triggered the nation's worst blackout. An official of the

organization that manages the flow of electricity across the Midwest, the Midwest Independent Transmission System Operator, cautioned Monday that system "contingencies" voltage increases and decreases are not unusual. But in this case they are being closely examined to see whether they might give a clue as to what triggered the cascade of power failures that hours later swept through lines from Michigan to New York City. **The industry investigation has focused on the likelihood of a combination of mechanical glitches and human failures as it tries to piece together second−by−second events during the hours before the widespread blackout, focusing on power lines in Ohio.**
Source: http://abcnews.go.com/wire/US/ap20030818_1098.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

6. *August 15, United States Department of Defense* — **Missile defense radar site chosen.** The Missile Defense Agency (MDA) announced today that it has selected Adak, Alaska, as the Primary Support Base (PSB) for the Sea−Based X−Band (SBX) radar. The SBX is a part of the Ground−based Midcourse Defense (GMD) system, a missile defense system designed to intercept and destroy long−range ballistic missiles aimed at the U.S. homeland. **The SBX will provide detailed ballistic missile tracking information to the GMD system, as well as advanced target and countermeasures discrimination capability for the GMD interceptor missiles.** The ability of the SBX to deploy to operating locations under its own power allows it to support actual GMD operations as well as realistic testing. The SBX is approximately 390 feet long and 250 feet high, and has a displacement of 50,000 tons.
Source: http://www.dod.mil/releases/2003/nr20030815−0373.html

7. *August 15, National Aeronautics and Space Administration* — **NASA and Navy sign memorandum of agreement. NASA and the U.S. Navy signed a Memorandum of Agreement to exchange valuable vendor and supplier information aimed at improving safety, mission assurance, and performance of the systems procured by both.** NASA Administrator Sean O'Keefe recognized many similarities between human space flight programs and submarine operations. Administrator O'Keefe wrote a letter to Navy Secretary Gordon England in July 2002, and in August 2002, the NASA/Navy Benchmarking Exchange Team was formed. This agreement allows NASA to use the Navy's Product Data Reporting and Evaluation Program and its Red/Yellow/Green Program, both of which are web−accessible to both organizations. NASA will provide the Navy with access to systems used to assess the quality of vendors and suppliers.
Source: http://www.nasa.gov/home/hqnews/2003/aug/HQ_03265_navy_mou.h tml

[Return to top]

Banking and Finance Sector

8. *August 18, Dow Jones Business News* — **'Phishers' use Citigroup logo in identify−theft attempt. Citigroup Inc.'s corporate logo is the latest one to be lifted by Internet scammers as a way to steal information from unwitting consumers. The scam involves "phishing,"** which is when thieves send consumers e−mails that appear to come from major corporations and direct them to bogus Web sites that look just like the company's real sites, and ask for customers' personal information. Citigroup said it is working with law−enforcement officials to investigate the fraudulent e−mails, adding it doesn't ask customers to provide sensitive information in this way. Citigroup is urging recipients of the e−mail to delete it immediately and report it to the company's customer−service department. **The banking giant also assured its systems haven't been compromised in any way.**
   Source: http://biz.yahoo.com/djus/030818/1407000809_2.html

9. *August 18, Banking Systems and Technology* — **Business continuity plans at work. Business continuity plans, designed to last through Y2K and battle−tested on September 11th, came to the fore during the power grid failure last week, thus limiting the initial impact to people in areas lacking electricity.** "Every bank in the country has, and is required to have, a disaster recovery plan and multiple backup systems," says Charlotte Birch, media spokeswoman at the American Bankers Association, Washington, DC. The result was a reported smooth transition for back−office processing throughout the financial system. "Banks really didn't miss a beat in terms of transitioning over to backup systems," says Birch. **Most members of the U.S. workforce received their mid−month direct deposits as usual, for instance, and credit card networks remained online.** For consumers located outside of the failed grid, transactions went through as usual, even when dealing with banks located in the affected area.
   Source: http://www.banktech.com/story/BSTeNews/BNK20030818S0003

[Return to top]

Transportation Sector

10. *August 07, Department of Homeland Security − Coast Guard* — **Safety and security zones; New York marine inspection zone.** The Coast Guard proposes to establish permanent safety and security zones in portions of the waters around La Guardia and John F. Kennedy airports in Queens, NY, the New York City Police Department (NYPD) ammunition depot on Rodman Neck in Eastchester Bay, the Port Newark and Port Elizabeth, NJ, commercial shipping facilities in Newark Bay, and between the Global Marine and Military Ocean Terminals in Upper New York Bay. **This action is necessary to safeguard critical port infrastructure and coastal facilities from sabotage, subversive acts, or other threats. The zones will prohibit entry into or movement within these areas without authorization from the Captain of the Port New York.**
   Source: http://a257.g.akamaitech.net/7/257/2422/14mar20010800/edocket.access.gpo.gov/2003/03−20023.htm

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

11. *August 18, Associated Press* — **EU defends biotech rules.** The European Union (EU) defended its rules for the sale of genetically modified foods Monday as the United States, backed by Argentina and Canada, asked the World Trade Organization (WTO) to overturn requirements they see as an unfair trade barrier. The 15 nation EU ended its moratorium on genetically modified (GM) food last month but said each product must undergo a scientific risk assessment and have a special label. **The United States, Canada and Argentina formally requested a dispute panel at the World Trade Organization to force the EU to approve GM foodstuffs unconditionally**. The European Union blocked the request for a special panel, but the U.S. is expected to raise the issue again on August 29 and the EU won't be able to block it again under trade rules. The EU defends its rules as a legitimate response to consumer concerns. If the U.S prevails at the WTO, the EU may have to allow imports of the genetically modified crops or compensate trading partners for banning them. The U.S. and others might be allowed to impose trade sanctions equal to the amount of sales lost during the European moratorium. **American farmers estimate the EU restrictions have cost them nearly $300 million a year in lost corn exports alone.**
    Source: http://www.kansascity.com/mld/kansascity/news/breaking_news/ 6560179.htm

12. *August 18, Associated Press* — **Hundreds of horses afflicted as mosquito virus cases rise. A mosquito−borne virus is spreading throughout the Southeast, afflicting hundreds of horses**. Florida has reported 178 horse cases of Eastern equine encephalitis, seven times last year's activity. The disease has infected 120 horses in South Carolina and 47 in Georgia, and has been reported as far north as Maryland. "This is the worst year in our records, it has hit the East Coast and the Gulf Coast pretty hard," said Dr. Venaye Reece, equine programs coordinator for Clemson University's livestock and poultry health programs office. **Nearly all horses infected with Eastern equine encephalitis either die or suffer severe brain damage.** Florida's virus activity may be showing signs of change. Last week Florida health officials recorded a drop in the number of new horse cases after weeks of increases, said Lindsay Hodges, spokeswoman for the Florida Department of Health.
    Source: http://www.bayarea.com/mld/cctimes/news/6558874.htm

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

13. *August 18, Las Vegas Review−Journal* — **New system for treating water supply exceeds expectations. Midway through a 30−day test period, the process known as ozonation is exceeding expectations at the Las Vegas, NV, water treatment plant. "It has improved the water's clarity by 10 times** of what it was before we started the system," said Ron Zegers, director of the Southern Nevada Water System. Although ozonation is effective at killing a variety of fecal bacteria, viruses, and giardia, the need to knock out the sometimes fatal parasite cryptosporidium is what spurred the effort to convert the treatment plant from reliance on chlorine as a disinfectant. "Chlorine could not eliminate cryptosporidium," Zegers said. He said a certain amount of chlorine still is required, by law, to be present in the system that delivers tap water to the valley. "There's always the issue of re−contamination in the distribution system, he said. Zegers said ozone is effective in killing cryptosporidium and other organisms because it breaks up their chemical bonds. **"The other thing we're beginning to find out is ozone oxidizes many of the pollutants and chemicals that might be used to contaminate a water supply," referring to the scenario of someone deliberately trying to spoil the water supply.**
    Source: http://www.reviewjournal.com/lvrj_home/2003/Aug−18−Mon−2003/news/21949349.html

14. *August 18, Detroit Free Press* — **Water still undrinkable. For the fifth day in a row, Detroit Water and Sewerage Department officials are asking their 4.3 million customers to boil all tap water before drinking it. Detroit sells water to 126 southeastern Michigan communities.** They also say residents should conserve water. Testing water in Michigan takes at least 48 hours. It requires two clear indications in a row that the water is clean. If both test results show bacteria−free water, the water's safe. **Thursday's power outage stopped the pumps, dramatically lowering the pressure and the amount of water in the pipes. That meant oxygen and bacteria were able to enter the water supply.** Detroit's water system has backup generators at three of its five plants that should kick in when the main power fails. **But the power wasn't nearly enough to get the water running at high pressures.** It was basically there for emergency reasons, like fires. In 1995, it cost $2 million in equipment alone to provide backup power for a plant that pumps 30 million gallons a day. Some of Detroit's plants pump 600 million gallons a day. **Victor Mercado, director of the water department said his department will closely examine what the department could have done differently.** But he's not sure whether the investments will be affordable.
    Source: http://www.freep.com/news/metro/water18_20030818.htm

[Return to top]

Public Health Sector

15. *August 18, New Scientist* — **Smallpox immunity. Vaccination may induce life−long immunity to smallpox, suggest the results of the first detailed tests of their kind.** In 1972, investigators found that people with a certain level of antibodies to the smallpox vaccine remained immune during outbreaks. An Oregon Health and Science University team has measured these antibodies in 306 people vaccinated between one and 75 years ago. Of those vaccinated 20 or more years ago, half still had antibodies at or above the protective threshold determined in 1972. One major question is if antibodies are the key factor in immunity. "The

assumption in recent years has been that immunity depends, not on antibodies, but on T−cells," said research team member Mark Slifka. The team found that such cell immunity does indeed wane after vaccination, with a half−life of eight to 15 years. In the test group, even people with little cell−mediated immunity left still had high levels of antibody. Taken together with the earlier observations, "this suggests that long−term smallpox immunity might depend on antibodies, not T−cells," says Slifka. **It suggests that half of those vaccinated as children, about one in four westerners, is currently immune to smallpox. Furthermore, nearly all of the rest of the vaccinated population may be partially immune.**
Source: http://www.newscientist.com/news/news.jsp?id=ns99994064

16. *August 18, Denver Post* — **West Nile treatment will get trial in Colorado. As early as this summer, Colorado residents might stand a better chance of surviving West Nile virus, thanks to injections of a smidgen of blood from Israelis who successfully fended off the potentially fatal infection. The National Institutes of Health funded trial with the Israelis' blood will play out at 35 sites across the nation where West Nile is expected to strike most ferociously this summer.** Already, one confirmed site is the University of Colorado Health Sciences Center, where an internal board is completing its review, one of the final hurdles before the trial can begin. The trial will use plasma from those West Nile survivors, treated so it doesn't pass along pathogens, to boost the immune systems of Colorado's most vulnerable West Nile victims. The so−called "passive immunization" with protective immunoglobulins is a potent weapon that's been used to combat a range of ailments, such as South American hemorrhagic fever and rabies.
Source: http://www.denverpost.com/Stories/0,1413,36~24167~1576720,00 .html

17. *August 18, National Institute of Allergy and Infectious Diseases* — **Promising West Nile virus vaccine. Scientists at the National Institute of Allergy and Infectious Diseases (NIAID) have created a promising vaccine against West Nile virus by replacing parts of a distantly related virus with proteins from the West Nile virus.** The NIAID research team replaced proteins in a virus known as dengue type 4 with the corresponding West Nile virus proteins, creating a hybrid virus vaccine that protects monkeys from West Nile infection. **Human clinical trials of the vaccine are expected to begin before the end of 2003.** "We're optimistic that our engineered virus vaccine will provide long−term immunity to West Nile virus, but the human clinical trials will give us the definitive data," says Brian Murphy, of the NIAID Laboratory of Infectious Diseases. The potential West Nile vaccine is a live but weakened virus. To create it, scientists took the dengue 4 virus and replaced its outer shell proteins with corresponding proteins from West Nile virus, explains Alexander Pletnev, lead investigator.
Source: http://www.eurekalert.org/pub_releases/2003−08/nioa−pwn08180 3.php

18. *August 18, Australian* — **Alert to biotech companies. Biotech companies have been warned to tighten their security because of increasing concern that commercially produced biological agents are falling into the hands of terrorists.** The rapid growth of the biotechnology sector, and greater global access to biological agents, equipment, and expertise were challenging national security, said Kylie Brown, of the arms control branch of the Australian Department of Foreign Affairs and Trade. Brown told a national biotech conference Friday the growth of the industry had brought with it a "dark side." Describing biological warfare agents as the "poor man's weapon", she said biotech companies needed to realize their potential role in accidentally supplying terrorists with weapons of mass destruction. **She said**

the industry should improve facility security, monitor the transfer of materials, technology and staff, and report thefts and unexplained losses of material. Michael Moodie, president of the Washington, DC−based Chemical and Biological Arms Control Institute, said the rapidly developing nature of biotechnology would outpace government regulation. This highlighted the need for an industry−led movement in which companies began taking responsibility for inadvertent involvement in terrorism.
Source: http://www.theaustralian.news.com.au/common/story_page/0,5744,6986939%255E2702,00.html

[Return to top]

Government Sector

19. *August 18, Government Executive Magazine* — **State Department issues new visa rules.** The State Department has issued two rules that aim to crack down on visa fraud and save the government money by streamlining the application process for a popular immigration program. **In March 2002, the department published an interim rule that denied the automatic visa re−validation privilege to foreigners from countries categorized by the U.S. government as state sponsors of terrorism. These countries include Iraq, Iran, Syria, Libya, Sudan, North Korea and Cuba. That rule also denied the benefit to those who chose to apply for a new visa while traveling in one of the United States'contiguous territories.** Monday's final rule is intended to protect against the possibility that automatic re−validation would enable those visa applicants who were eventually rejected to return to the United States while their applications were pending. The final rule, which goes into effect August 18, mirrors the 2002 interim rule. It does not preclude foreigners who are in the U.S. and plan to go abroad temporarily from applying for a new visa prior to leaving this country. **The department emphasized that the visa benefit was a privilege, not a right, and the changes reflect a post−September 11 world. "These are difficult and different times, and certain conveniences must be foregone," the rule stated.**
Source: http://www.govexec.com/dailyfed/0803/081803m1.htm

[Return to top]

Emergency Services Sector

20. *August 18, Chicago Sun Times* — **Outage disrupts New York, Detroit 911. Last week's blackout disrupted emergency dispatch systems in two major cities, leaving 911 operators in Detroit hand−writing notes to distribute to police officers on the streets and cutting communications between New York dispatchers and personnel for spans as long as 14 minutes, officials acknowledged Sunday.** The three extended New York disruptions−−of 14, 11 and 7 minutes−−did not affect incoming 911 calls from the public, but they cut off normal communication between dispatchers and personnel on the street, said fire department spokesman Mike Loughran. Residents in Detroit could also make emergency 911 calls during the two−hour computer failure, but the computer−assisted dispatch system normally used by operators to record the calls and dispatch the appropriate responders was down, said Jamaine Dickens, a spokesman for Mayor Kwame Kilpatrick. **The Detroit operators were left to write**

out the details of the calls on paper and distribute the information by hand to police, fire and emergency medical service dispatchers, but there appeared to be little impact on the response, Dickens said. The problems in New York weren't critical, and city officials said no 911 calls were completely lost, but the city will investigate, New York Mayor Michael Bloomberg said Sunday.
Source: http://www.suntimes.com/output/news/cst−nws−blackout18.html

21. *August 18, Stateline.org* — **Northeastern states seek terrorist intelligence sharing. Homeland security officials in 10 northeastern states want to establish intelligence−sharing centers that would better disseminate terrorist−related information between federal law enforcement and local police officers.** Mark Cohen, director of the New York State Office of Public Security, said the ability to share intelligence with the federal government in real time is "the most critical component for homeland security in the states." **Cohen and homeland security officials in nine other states have asked Congress and the U.S Department of Homeland Security (DHS) to establish intelligence−sharing centers in the Northeast that would give police access to federal databases containing information on individuals with terrorist links as well as other related intelligence.** The system would be based at the New York Intelligence Center in Albany, which currently connects all law enforcement agencies in New York. **Under a pilot program proposed to the U.S. Department of Homeland Security, the system would expand to connect law enforcement agencies in every northeastern state, from Maine to Delaware, with the federal government,** Cohen said.
Source: http://www.stateline.org/story.do?storyId=321075

[Return to top]

Information and Telecommunications Sector

22. *August 18, Government Computer News* — **Emergency telecom programs gave responders access. Priority services operated by the National Communications System (NCS) gave government officials and emergency personnel access to both landline and wireless telecommunications during the blackout** that shut down parts of the Northeast Thursday and Friday. Although most of the telecommunications infrastructure remained in operation, usage spikes overwhelmed resources, making access difficult for many calling to or from the affected areas. That is the situation for which the Government Emergency Telecommunications Service (GETS) was established for landline phones, and the Wireless Priority Service (WPS) for cellular phones. GETS gives priority users access to the public−switched network. WPS gives priority to calls by federal, state and local officials and industry first responders who dial a special cellular system. **Routine calls are not dropped, but priority calls are moved to the head of the queue waiting for a channel on the nearest available cell**.
Source: http://www.gcn.com/vol1_no1/daily−updates/23184−1.html

23. *August 18, Washington Post* — **FCC vows to fix radio interference.** The explosive growth of the mobile phone industry has crowded and tangled the nation's airwaves to such an extent that **wireless company signals are increasingly interfering with emergency radio frequencies used by police and firefighters**, public safety agencies said. Emergency departments across the country report many stories of officers who can't call for backup, dispatchers who can't

relay suspect descriptions and firefighters who can't request ambulances because of radio "dead spots" believed to be caused by wireless phone interference. To solve the problem, **the Federal Communications Commission (FCC) is considering reshuffling channels in the 800 megahertz band, which potentially could cost hundreds of millions of dollars** and take years to complete, industry officials said. The idea is to separate the wireless companies from the public safety departments, so they inhabit different ends of the band.
Source: http://www.washingtonpost.com/wp−dyn/articles/A7270−2003Aug1 7.html

24. *August 18, U.S. Department of Homeland Security* — **New version of the MS−RPC DCOM Worm infecting machines and creating Denial of Service Conditions.** A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi", "welchia", or "msblast.d" does not infect systems that have been updated to counter the Blaster worm but will re−infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. **The variant then begins scanning or flooding the network with high volumes of ICMP (Internet Control Message Protocol) traffic causing network congestion which can result in denial of service conditions**. Users should patch the MS−RPC DCOM vulnerability immediately using the instructions available on the Microsoft Website: http://www.microsoft.com/security/incident/blast.asp.
Source: http://www.nipc.gov/warnings/advisories/2003/Advisory8182003 .htm

25. *August 17, Gulf News* — **Power cut shifts focus to cyber security. Last week's blackouts showed how vulnerable our society is to disruption of such complex systems as the power grid**. U.S. intelligence officials last year discovered an al Qaeda safe house in Pakistan devoted to training people for computer hacking and cyber warfare where al Qaeda operatives gathered information on the automated systems that control U.S. infrastructure, such as dams and power grids. The terrorists haven't yet demonstrated the capacity to carry out large−scale terror, but that doesn't mean they haven't achieved the necessary level of expertise to do it. This situation is alarming when one considers that **America has many thousands of dams, airports, chemical plants, federal reservoirs and power plants (of which 104 are nuclear), most of whose integral systems are controlled by sophisticated computer systems** or other automated controllers.
Source: http://www.gulf−news.com/Articles/Opinion.asp?ArticleID=9536 4

26. *August 15, National Journal* — **Congress lowers funding for intelligence, cybersecurity. The Senate Homeland Security Appropriations Committee awarded the Department of Homeland Security's information analysis and infrastructure protection directorate $823.7 million for fiscal 2004. It would use the money to collect and disseminate information on terrorist threats, integrate data with foreign intelligence agencies, and develop and implement a plan against terrorist threats and national vulnerabilities**, according to the Senate committee. The Senate approved $98.5 million to monitor and coordinate work on cyber−security infrastructure, including the creation of a national cyber−security division. Some $33 million would be available for advisories, and $66 million would go for cybersecurity from funds available for remediation and protective actions. The Senate also offered $294 million to guide the development of protective measures for critical infrastructure and $155 million for the National Communications System to expand

telecommunications capabilities for national security and emergency preparedness.
Source: http://www.govexec.com/dailyfed/0803/081503td2.htm

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 3 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 445 (microsoft−ds), 137 (netbios−ns), 1434 (ms−sql−m), 443 (https), 27374 (SubSeven), 80 (www), 139 (netbios−ssn), 4444 (CrackDown), 1433 (ms−sql−s) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *August 18, The Associated Press* — **Australia, U.S. may practice WMD searches at sea.** Joint Australian−U.S. naval exercises scheduled for next month may be used to practice boarding vessels suspected of exporting weapons of mass destruction from rogue states, the Australian government said Monday, August 18. **Officials from the United States, Australia, Japan and eight European countries − agreed in principle last month to begin training for high seas "interdictions" of ships believed to be carrying weapons of mass destruction.** No date has been given for the first exercises next month in the Coral Sea off Australia's northeast coast. "The government is considering using the maritime component of the routine bilateral Exercise Crocodile 03 scheduled for September in the Coral Sea as a potential opportunity to conduct this type of training," the Australian Defense Department said in a statement, referring to the possible maritime interdictions.
Source: http://www.usatoday.com/news/world/2003−08−18−australia−us_x .htm

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer